AN ANALYSIS OF BIOMETRIC TECHNOLOGY AS AN ENABLER TO INFORMATION ASSURANCE

THESIS

Darren A. Deschaine, Master Sergeant, USAF

AFIT/GIR/ENV/05M-03

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GIR/ENV/05M-03

AN ANALYSIS OF BIOMETRIC TECHNOLOGY AS AN ENABLER TO
INFORMATION ASSURANCE

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Darren A. Deschaine, BS

Master Sergeant, USAF

March 2005

AFIT/GIR/ENV/05M-03

AN ANALYSIS OF BIOMETRIC TECHNOLOGY AS AN ENABLER TO
INFORMATION ASSURANCE

Darren A. Deschaine, BS
Master Sergeant, USAF

Approved:

/signed/	28 Feb 05
Captain David D. Bouvin, PhD, (Chairman)	Date
/signed/	4 Mar 05
Dr. Kevin L. Elder (Member)	Date
/signed/	28 Feb 05
Dr. Dennis D. Strouble (Member)	Date

AFIT/GIR/ENV/05M-03

Abstract

The use of and dependence on Information technology (IT) has grown
tremendously in the last two decades. Still, some believe we are only in the infancy of
this growth. This explosive growth has opened the door to capabilities that were only
dreamed of in the past. As easily as it is to see how advantageous technology is, it is also
clear that with those advantages come distinct responsibilities and new problems that
must be addressed. For instance, the minute we began using information processing
systems, the world of information assurance (IA) became far more complex as well. As a
result, the push for better IA is necessary. To reach this increased level of IA, a further
dependence on technology has developed. As an example, the field of biometrics has
matured and has become an enabler to the United States Department of Defense IA
model.

Acknowledgments

      First, I would like to express my sincere gratitude to God in heaven without whom I could not have made it through this program.

      Next, I must express appreciation to my thesis committee for their dedication to this effort. Special thanks to Captain Dave Bouvin, my committee chair, for keeping me focused and on track during this process. Your guidance allowed me to explore and learn much more than this document details. To Dr. Kevin Elder and Dr. Dennis Strouble, my readers, you have my sincere appreciation helping me complete this effort. Also, to the ENV faculty for their direction and patience during the last eighteen months, you have my gratitude. You each contributed significantly and taught me to look for meaning beyond mere face value. And to my fellow IRM classmates, you are each a source of inspiration and it has been a pleasure sharing this experience with all of you.

      CMSgt Wallace Simmons (Ret.), you have been more of a mentor and a leader than you know. Thank you for believing in me and guiding so many of us over the years. You are an exceptional man who exemplifies our Air Force core values. When I think of integrity, service, and excellence, your name will always come first.

      Lastly, but certainly not least, I could not have made if through this program without the constant support of my family and friends. You may never know what an unending source of strength and motivation you are to me. Thank you from the bottom of my heart.

                                 Darren A. Deschaine

Table of Contents

List of Figures

List of Tables

AN ANALYSIS OF BIOMETRIC TECHNOLOGY AS AN ENABLER TO
INFORMATION ASSURANCE

I. Introduction

Background

Information technology (IT), in both the hardware and software realm, has grown

tremendously in the last two decades. This explosive growth has opened the door to

capabilities that were only dreamed of in the past. Even with the incredible developments

we have already been privileged to see and employ in our daily lives, some believe we

are still in the infancy of this growth. And, as easily as it is to see how advantageous

technology is, it is also clear that with those advantages come distinct complications and

responsibilities. For instance, the minute we began using information processing systems,

the world of information assurance (IA) became far more complex as well. As a result,

the push for better IA has taken on new focus.

Problem Statement

The role and use of IA in the modern environment cannot be understated.

Technology is growing so quickly that it can often be difficult for information technology

(IT) mangers to keep up. Protecting our information systems and the invaluable data and

information they contain has become a critical focus area for IT professionals. But, as

technology dependence increases, so too does our vulnerability. Often, managers look

toward technology to address these weaknesses. Using technology to solve technological

problems can open the door to additional problems. For example, employing strong

counter measures can often require computing power and expertise only achievable by

further dependence on IT. As our IA challenges grow, managers look for new ways to address the growing concerns. One field of endeavor, biometrics, has garnered much attention in recent years. This field has much potential and could prove to be one area where technology is helping to solve some problems. But, to be valuable, these technological developments must contribute positively to some area of interest. One such area is the IA arena.

Research Focus and Objectives

The focus of this research effort will be to investigate the broad conceptual framework of IA, to examine the necessary components of a strong IA program, and to explore the need for a comprehensive IA model and initiative.

In addition, the field of biometrics will be investigated. A generalized overview of the science of biometrics will be looked at and an analysis of the technologies available for use will be examined. This, in turn, will be followed by an investigation of the applicability they have to the concepts of the Department of Defense (DOD) IA model.

Finally, the relationship that exists between IA and biometrics will be explored and a synthesis of facts, ideas, and thoughts will be presented

Research Question

The focus of this research effort will be to determine if the recent explosion of biometric technology has contributed positively to the realm of IA. For the purpose of this research, the research question to be answered will be:

- In what manner, if any, does the use of biometric technologies act as an enabler to information assurance?

Investigative Questions

In order to effectively answer the research question at hand, it will be necessary to answer several investigative questions. During the research process, the following investigative questions will be explored:

1. What components are considered critical to the DOD IA model?

2. What advantages do biometric technologies provide that may contribute positively to IA efforts?

3. What concerns have been raised regarding the use of biometric technologies that may hinder IA efforts?

4. Which components of the IA model can be addressed by the use of biometric technologies?

The answers to these investigative questions will allow the researcher to draw conclusions and answer the main research question.

Methodology

An historical research methodology will be used in this research effort. A thorough review of applicable literature will be collected and evaluated in the context of an historical research framework. Multiple libraries and literature databases will be searched in an effort to discover peer reviewed literature as well as applicable government publications applicable to this effort.

Assumptions/Limitations

The IA model as detailed in DOD Joint Publication 3-13 (1998) will be used as a foundational framework for this research effort. Identification of key components of the IA model and their associated definitions vary among publications and literature. In fact, some publications do not acknowledge all components of the DOD IA model as being critical. Therefore, it should be noted that this research effort is focused on the components and definitions provided in the DOD literature.

The science of biometrics is a vast field of endeavor. Each technology in use could easily be considered a separate field of study. However, to study each technology intimately is beyond the scope of this research. This research is not intended to address all issues, concerns, or endeavor for each technology. Rather, this effort will introduce the technologies and attempt to provide an overview of those technologies as they relate to the overarching concept of the IA model.

Additionally, an historical research methodology will be used for this effort. This methodology, as with all methodologies, has inherent limitations. Due to the fact that the historical methodology uses the researcher as the instrument of investigation, researcher biases and values, although limited to as large a degree as possible, can be assumed to influence interpretation of the data (Leedy & Ormrod, 2001). Further limitations to the historical methodology will be discussed in detail in Chapter III.

Implications

This study will attempt to make a connection between the existing DOD IA model provided in the DOD publications and the use and perceived increasing popularity of

biometric technologies. The study will also determine whether or not the use of

biometrics, as a means of identification or authentication, supports the components

integral to an effective DOD information assurance effort.

II. Literature Review

Chapter Overview

The purpose of this chapter is to introduce and define information assurance (IA) and to explain the importance and need for a comprehensive IA plan in today's complex information systems environment. Additionally, this chapter will introduce the technology of biometrics, define several types in use today, and present information important for anyone considering the use of these technologies as part of their information systems security strategies.

Description

In the world of the computer age, information moves at incredible speeds. Computing power continues to grow and this provides us with fantastic opportunities only dreamed of in the recent past. However, while this explosion in technology allows us to develop the good, there are those among us that embrace the chance to explore the bad. In an effort to address these issues, a focus on IA becomes a necessary part of the equation.

Information Assurance (IA) Defined

Information assurance (IA) has become a necessary function in the information systems community. Threats to these systems and their valuable information are real and cannot be ignored. Out of the need to protect our systems and information, the field of IA has become critical. However, to understand IA in the DOD context, we must first look at the bigger picture to what the DOD calls Information Operations.

Information Operations (IO) encompass actions taken to affect the information or information systems of our enemies while at the same time protecting our own (DOD JP3-13, 1998). It is through IO that we hope to achieve and maintain the information superiority so critically needed by our military fighting forces. IO can and must take form in many shapes but can broadly be classified into two sub-categories: offensive information operations and defensive information operations.

Offensive IO are classified as those operations conducted to influence or affect adversary decision makers in an effort to promote our own objectives (DOD JP3-13, 1998) .this can include such activities such as electronic warfare, operations security , or military deception to name a few (DOD JP3-13, 1998).

Defensive IO, on the other hand, are those operations, policies, and procedures we use to protect and defend our own information and information systems. These include such initiatives as physical security, counterintelligence, electronic warfare, and information assurance (DOD JP3-13, 1998). These activities ensure our own access to these critical resources while at the same time, denying our adversaries the ability to exploit them for their own use (DOD JP3-13, 1998).

Taken in this context, it is important to realize just how significant IA is to the overarching concept of IO and information superiority. It is no secret that the DOD is a large proponent of IA. Considering the size of the DOD and its military components, the dependence that has grown on information systems, the adversaries that threaten those systems, and the need to protect these systems, IA is not just a nicety; it is a necessity. The DOD defines IA as:

"Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." (DODI 8500.2, 2003, p. 19; DOD JP 3-13, 1998:GL7)
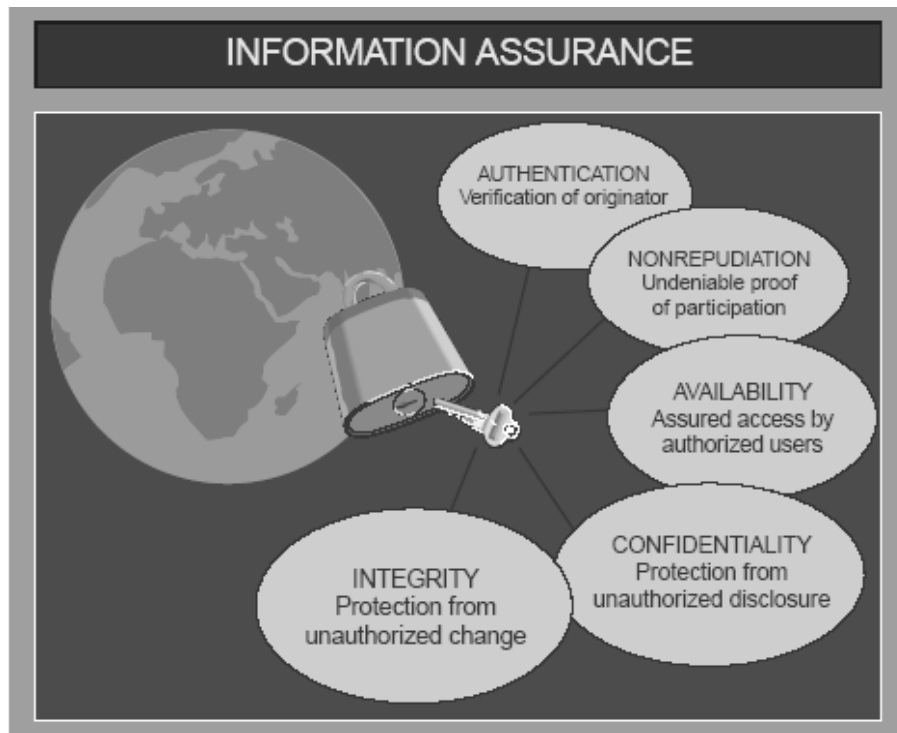
Figure 1: Key Components of IA
Source: (DOD JP 3-13, 1998)

In fact, the DOD directs that all DOD information systems are required to uphold appropriate levels of five distinct attributes in an effort to strike a balance between the usefulness, sensitivity, and importance of the system and the data or information it contains (DODD 8500.1, 2002). This is an incredibly large undertaking. Entire fields of endeavor have been spawned trying to address even a single aspect of these five components. Additionally, confusion can exist between IT terms such as IA, information security, and physical security. While they sound quite similar, they do in fact attempt to

define separate and distinct pieces of the puzzle, each with a unique focus. Therefore, to

help alleviate some of the confusion, it is necessary to explain the difference between

these closely related terms.

Information Security (INFOSEC)

IA and information security can be easy to confuse. While both are concerned

with intentional and unintentional attacks (Blyth & Kovavich, 2001), INFOSEC can be

thought of as a subset of IA focused primarily on the information and those systems that

process that information. Information Security can be defined as:

> "The protection of information and information systems against unauthorized
> access or modification of information, whether in storage, processing, or transit,
> and against denial of service to authorized users. Information security includes
> those measures necessary to detect, document, and counter such threats.
> Information security is composed of computer security and communications
> security." (DOD JP 3-13, 1998:GL-7; DOD JP 1-02, 2001:257)

While the difference is subtle, it is one worth noting. INFOSEC is concerned with

unauthorized access or modification of information. The focus of IA is larger in scope

and does not stop at unauthorized access or modification. Rather it addresses other key

components as well.

Physical Security

Physical security can be thought of as an external line of defense and is defined

as:

> "That part of security concerned with physical measures designed to safeguard
> personnel; to prevent unauthorized access to equipment, installations, material,
> and documents; and to safeguard them against espionage, sabotage, damage, and
> theft". (DOD JP 3-13, 1998:GL-9; DOD JP 1-02, 2001:409)

9

Careful examination of this definition shows concern for the tangible access to the information system more than the information itself. Physical security can be accomplished via numerous methods, including the use of secure facilities, access control systems to information system areas, and physical identification and authentication control systems to name a few. Preventing access to the system itself can often preclude loss, corruption, theft, or manipulation of the information and data it contains.

The Need for IA

Information systems touch our lives in ways many of us may not realize. It is easy to take for granted the conveniences technology provides, especially once those conveniences have become the norm. How many of us really consider what transpires behind the scenes when we make a bank withdrawal from an automated teller machine, perform an online transaction, or make a purchase with a credit card? Information systems are required to distribute the utilities to our homes and to manage the health care, financial, and transportation industries we have come to depend on. It is modern information systems that make these things possible. It only stands to reason that these systems need protecting.

No system can be considered completely secure. Computer crime is a problem that is not likely to go away and must not be ignored. With the number of information systems and users on the rise, it is important to understand that the problem will continue. Strategies to mitigate these problems should be employed.

The Computer Security Institute, in conjunction with the Federal Bureau of Investigation (Computer Crime Squad, San Francisco), has conducted a computer crime

and security survey for the last 9 years. The 2003 CSI/FBI survey showed that 56% of

survey respondents reported unauthorized use of computer systems within the 12 months

prior to the survey (CSI/FBI, 2003). In the 2004 survey, that figured declined to 53%

(CSI/FBI, 2004). And while a downward trend is present for the yeas 2000 – 2004, a

significant amount of unauthorized access, over 50%, is still present. Figure 2 below

details a side by side comparison of the years 1999 - 2003.
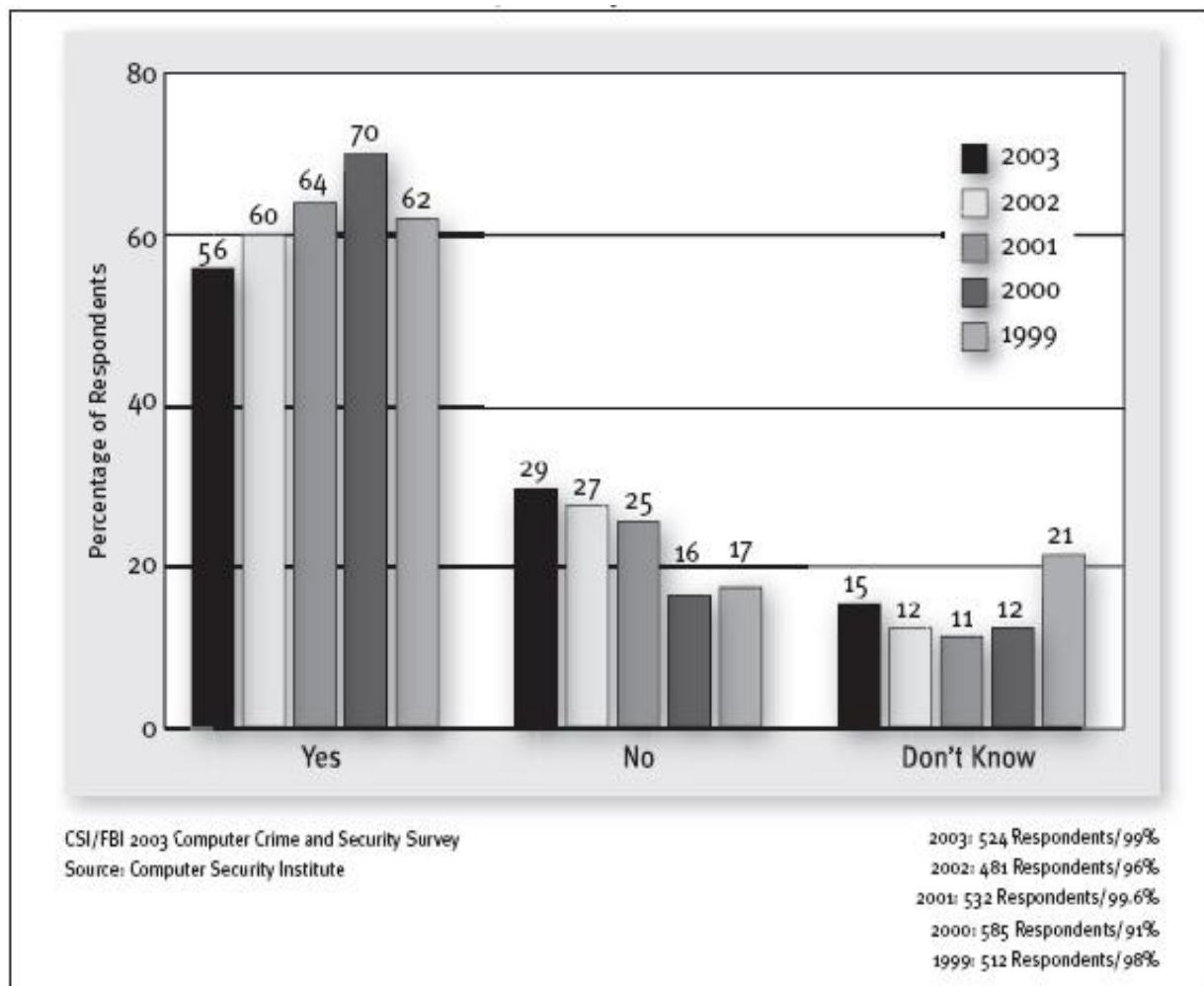
Figure 2: Unauthorized Use of Computer Systems
(Source: CSI/FBI Survey, 2003)

Achieving IA

There is no surefire method for achieving ideal IA. In fact, some say that perfectly secure systems do not exist. There are, however, methods to mitigate the risks associated with the use of technology. Technology itself provides some of the very tools we need. The 2003 CSI/FBI Computer Crime Survey shows security technologies and methods in use from 1999-2003.

Security Technologies Used
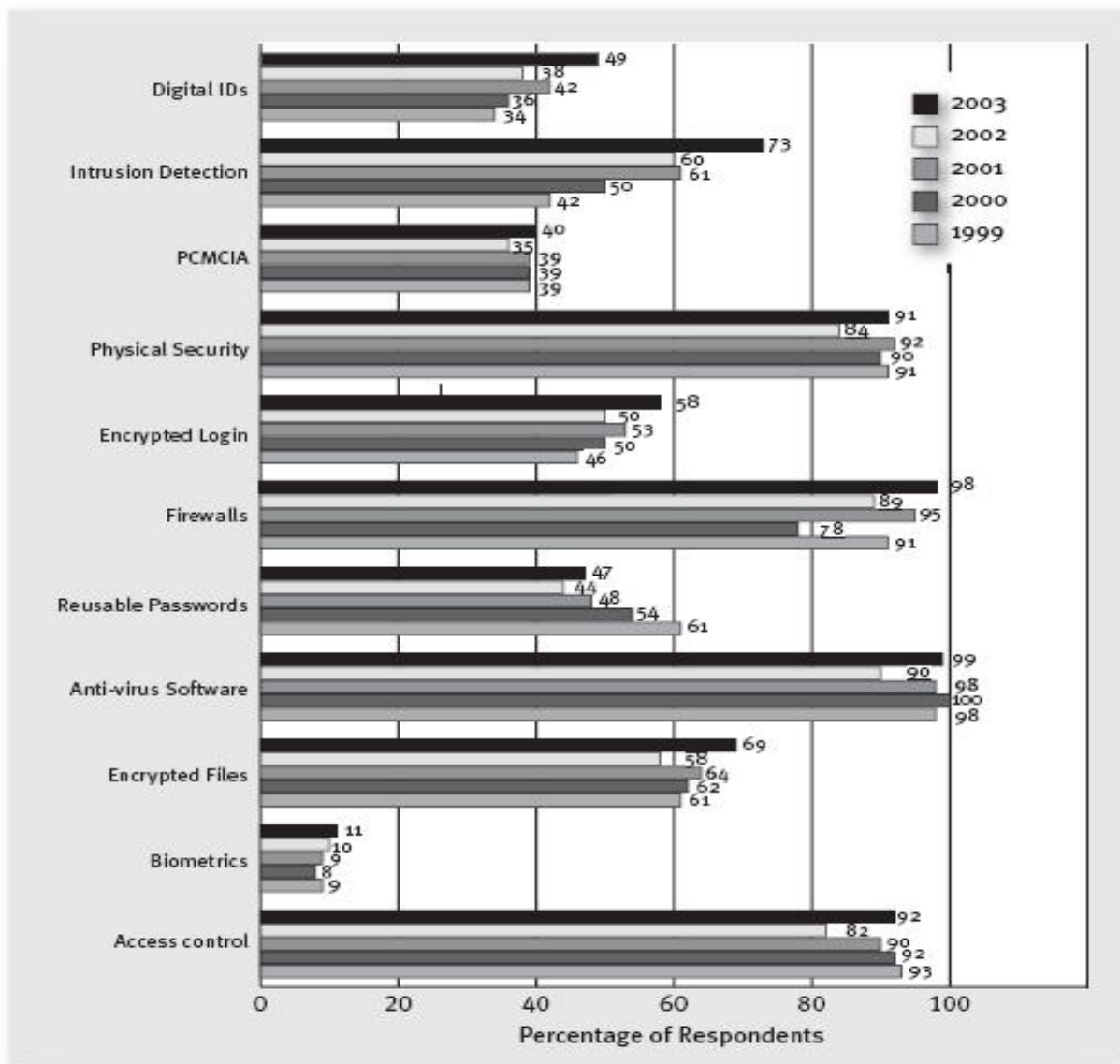
Figure 3: Overview of Security Technologies in Use
(Source: CSI/FBI Survey, 2003)

It is clear to see that a variety of methods are being employed to address the issue of

security. For example, while only 11% specifically admitted to including some form of

biometric technology in their efforts, it demonstrates a willingness to use additional technology to address technological problems.

Addressing the IA Model

As indicated in the previous section, there are five key components to the DOD IA model: authentication, non-repudiation, confidentiality, availability, and integrity. To achieve IA, we must address each of these individually. Therefore, it is important to take a closer look at each.

Authentication – The ability to be able to verify the originator (DOD JP 3-13, 1998:GL-9; DOD JP 1-02, 2001:409). Cummings (2002) goes further and explains that authentication establishes validity by ensuring a transaction occurred from a known source (Cummings, 2002). Using a less than secure authentication system could result in consequences such as compromise, loss of information or integrity, or even denial of service (Ratha, Connell et al., 2001).

Historically, authentication systems have employed various methods. Many experts (Liu & Silverman, 2001; Matyas & Riha, 2003; O'Gorman, 2003; Ortega-Garcia, Bigun et al., 2004; Ratha, Connell et al., 2001; Reid, 2004; Ribaric, Ribaric et al., 2003; Seno, Sadakane et al., 2003) agree that these methods have included three main items:

- *Something you know* – This is generally a password or personal identification number (PIN) that is supposed to be kept secret and known only to the authorized user.

- *Something you have* – This is generally a token of some sort, usually a pass card or a smart card that only the authorized user is supposed to possess.

- *Something you are* – This is a biometric identifier that uniquely distinguishes the authorized user.

Non-repudiation – Undeniable proof of participation (DOD JP 3-13, 1998:GL-9; DOD JP 1-02, 2001:409). In other words, irrefutable evidence exists to say that an action or transaction has taken place. This is often accompanied by some sort of time stamp or similar indicator (Cummings, 2002).

Availability – Assured access from unauthorized users (DOD JP 3-13, 1998:GL-9; DOD JP 1-02, 2001:409).

Confidentiality – Protection from unauthorized disclosure (DOD JP 3-13, 1998:GL-9; DOD JP 1-02, 2001:409). If sensitive information were to fall into the wrong hands, it could be catastrophic. Ensuring confidentiality means that information is only disclosed to an intended recipient (Cummings, 2002).

Integrity – Protection from unauthorized change (DOD JP 3-13, 1998:GL-9; DOD JP 1-02, 2001:409). An integrity check lets the receiver know that the information has not been altered in any way since the original creation and during the transmission or delivery process (Cummings, 2002).

Biometrics

The science of biometrics has garnered a lot of attention as of late. This science, while some forms of it have been around for decades, is still relatively young. So, what is biometrics?

According to Bolle et al, "Biometrics is the science of identifying, or verifying the identity of, a person based on physiological or behavioral characteristics." (Bolle, Connell et al., 2004). While at first glance this might seem unusual to some, many of us do it everyday. For instance, we almost unconsciously notice a person's size. Through the years, man has identified and taken notice of these individual characteristics (Adhami & Meenen, 2001). By creating systems that can capture and evaluate them, we have been able to use them as a form of identification and authentication. A biometric system is a recognition system that can verify the legitimacy and authenticity of a specific physiological or behavioral characteristic of a user (Jain, Bolle et al., 1999; Jain, Hong et al., 2000; Jain, Ross et al., 2004). Breaking these definitions down a little further, two key words are noticeable: physiological and behavioral.

What is the difference between the two? Physiological refers to those characteristics that are part of a person's physical make-up. Fingerprints are an excellent example of a physiological biometric. Physiological biometrics, by their very nature of being something a person is, remain relatively unchanged throughout a person's lifetime. An exception to this, of course, is the case where a characteristic altering injury such as loss of a finger, has occurred.

Behavioral characteristics, on the other hand, focus on the way an action is carried out. Signature and voice capture biometrics are good examples (Bolle, Connell et al.,

16

2004). One interesting area of note, behavioral characteristics can be influenced more by controllable actions and unintentional psychological factors (Miller, 1994).

The Basics of Biometric Systems

Investigating biometric systems, we can envision two main reasons to employ such a system: to identify a person or to verify an identity (Gamassi, Lazzaroni et al., 2004; Jain, Bolle et al., 1999; Phillips, Martin et al., 2000). Although these sound similar, they are distinctly different.

Identification systems are used when a person's identity is unknown. If we wish to find out who a person is, we must compare their biometric to a database of records to see if a match can be made. This is called one-to-many (1:N) comparison (Jain, Bolle et al., 1999; Nanavati, Thieme et al., 2002). As you can imagine, a system of this nature could require a large number of resources to identify even one person. Consider a database of 100,000 records. In an effort to make a match, the system would need to compare the captured biometric to all records.

In contrast, when using a biometric system as a verification system, the user identifies him or her self along with providing a biometric sample. A comparison is then made to one record on file in an attempt to verify that person's identity. This is called a one-to-one (1:1) comparison (Jain, Bolle et al., 1999; Nanavati, Thieme et al., 2002).

Another distinguishing feature can be made between systems. Some systems are considered to be positive identification systems while others are negative. This refers to whether or not we are looking to make a match. For example, some systems are designed to ensure that a person is not in a database. This is called a negative identification system.

17

This type of system can prevent people from enrolling in the same system multiple times (Nanavati, Thieme et al., 2002).

So, how do biometrics systems work? While each system is technologically different, the basic premise is similar throughout.

How a Biometric System Works

In order for a biometric system to work, some critical steps must take place. First and foremost, a user's biometric data must be captured, stored, and processed into a form the system will be able to readily use. To do this, a user presents a sample of the biometric to be measured and captured. The sample is converted to a mathematical representation of the information (Gamassi, Lazzaroni et al., 2004) and is stored in the form of a template. This process is often referred to as enrollment (Nanavati, Thieme et al., 2002). It is this template that the system will later use to determine a biometric match.

Next, for a user to authenticate with the system, they must again present a sample to a hardware capture device. Once the sample has been acquired by the interface, the raw data is converted to a template and sent to the verification system for comparison to the enrollment data. (Nanavati, Thieme et al., 2002)

The two templates are then compared and a score, based on the degree of similarity or correlation, is generated. If the score falls within the allowable threshold, a decision to accept is made. Naturally, if the score is not within the specified threshold a decision to reject is made (Gamassi, Lazzaroni et al., 2004). In the case of a reject, the

user may be prompted to submit another sample for further verification.(Nanavati,

Thieme et al., 2002)

The Ideal Biometric System and Potential Errors

Can an ideal biometric system, or any identification or authentication system,

really exist? It is difficult to say. However, Phillips et al. (2000) say that for an ideal

biometric system to exist, the following must apply:

- All members of the population must possess the characteristic biometric,

   i.e. a fingerprint.

- Each biometric must differ from all others in the population. In other

   words, each signature must be unique.

- No variation exists between methods of collecting signatures.

- The system must be capable of resisting countermeasures (Phillips, Martin

   et al., 2000).

Jain et al. (2004) and Prabhakar et al. (2003) refer to four similar traits as universality,

distinctiveness, permanence, and collectability. These can be defined as:

Universality – Each person should possess the required characteristic.

Distinctiveness – Any two people should be suitably diverse for the same

   characteristic.

Permanence – The characteristic should be invariant over time.

Collectability - The trait can be measured quantitatively.

Furthermore, three additional requirements that should be considered: performance, acceptability, and circumvention (Jain, Bolle et al., 1999; Jain, Ross et al., 2004; Prabhakar, Pankanti et al., 2003). Jain (1999, 2004) defines these as:

Performance - recognition accuracy and speed, as well as the resources (including environmental factors) to achieve the required accuracy and speed.

Acceptability – the degree to which people will accept the technology and its use.

Circumvention – the degree to which the system is easily evaded or outsmarted.

It is only practical to evaluate biometric systems using these characteristics. All biometric technologies are different and possess their own unique traits and challenges. Because of this, a delicate balance exists between those traits and challenges.

In spite of their disparity, however, a few common errors do exist between systems and should certainly be anticipated. As indicated by multiple experts (Ashbourn, 2004; Golfarelli, Maio et al., 1997; Matyas & Riha, 2003; Phillips, Martin et al., 2000; Ratha, Connell et al., 2001), common errors include:

- *Failure to Enroll (FTE)* – This error occurs when a user cannot provide a biometric template to the system that can be successfully converted to a usable template. This could be due to reasons such as a physical disability of degradation of the biometric trait.

- *False Accept Rate (FAR)* - False accept rate (also referred to as type II error) is the term given to the probability (or sometimes percentage) of error that occurs when a template is presented and falsely accepted as matching an authorized template. In this case, an imposter has gained access to the system.

- *False Reject Rate (FRR)* – False reject rate (also referred to as type I error) refers to the probability (or sometimes percentage) of error that occurs when an authorized sample is presented but is incorrectly rejected by the system as unauthorized. In this case, an authorized user cannot gain access.

Figure 4 below demonstrates the relationship between FAR and FRR
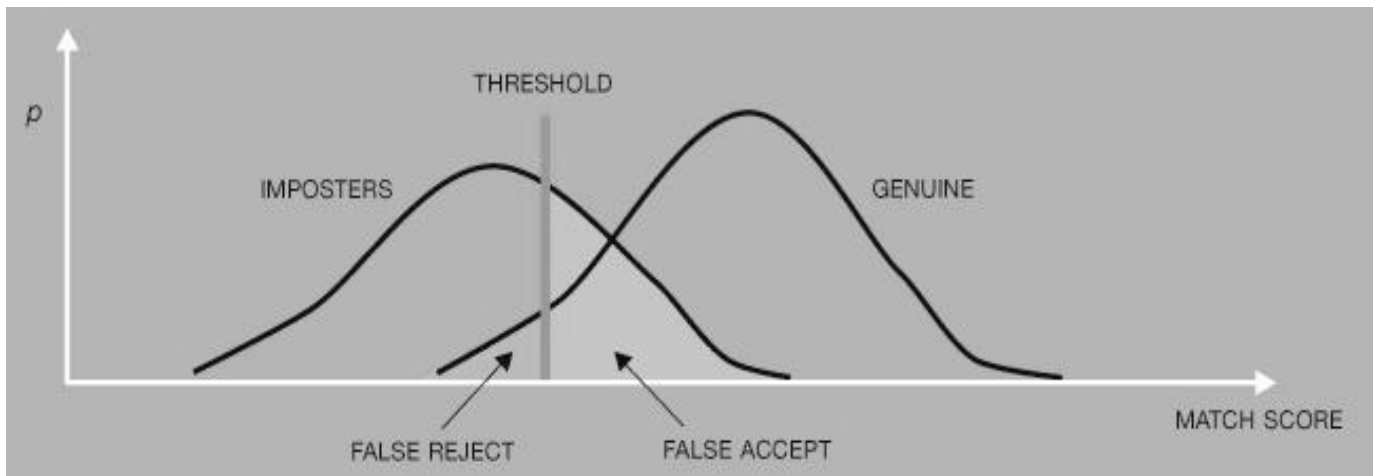
Figure 4: Error Trade-off in a Biometric System
Source: (Ratha, Connell et al., 2001)

- *Crossover Error Rate (CER)* – This refers to the error rate at which the FAR equals the FRR; the lower the CER, the better the device. A pictorial representation of this relationship can be seen below.
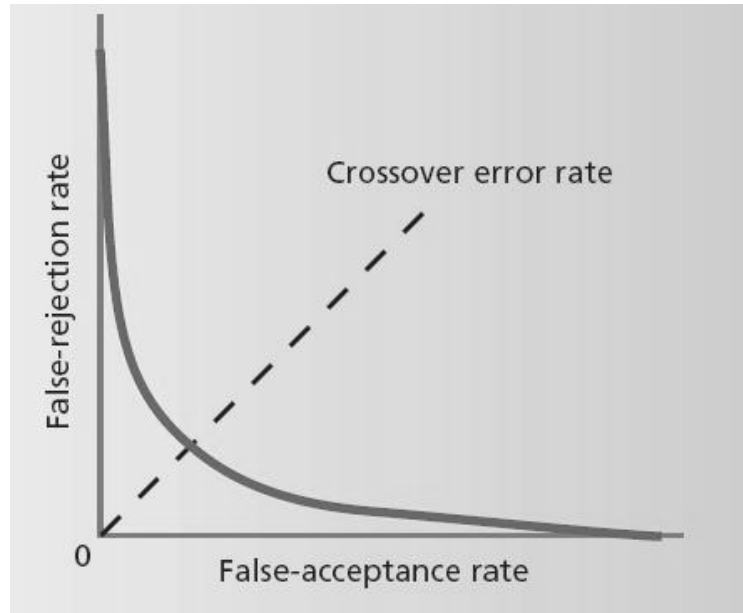
Figure 5: Crossover Error Rate (CER)
Source: (Liu & Silverman, 2001)

Additionally, time and environmental conditions can cause errors to biometric data as

well (Liu & Silverman, 2001). Over a series of time, in some instances, some biometric

characteristics, while relatively stable, can change. The human aging process is an

excellent example of this effect (Liu & Silverman, 2001). Also, environmental

conditions, such as interference, noise, or other outside influences can affect the

collection of a sample.

Figure 6 below gives an excellent illustration of the process described above.

Again, while not all systems operate exactly the same way, this process provides a good

general overview of what happens in a biometric authentication system.

Figure 6: Basic Process Flow: Biometric Matching
(Nanavati, Thieme et al., 2002)

Common Forms of Biometric Technology

There are many forms of biometric technology on the market. In order to get a better understanding of these technologies, how they work, and how we might take advantage of them, a closer examination is necessary. With this in mind, a short discussion of several of the more common technologies and their individual characteristics is appropriate.

Fingerprints

Possibly the most commonly known type of biometric is the use of fingerprints. The science of fingerprinting relies on the concept that no two people have identical fingerprints, even among fingers on the same hand. This allows for a unique identifier for

23

each individual. This may partially explain why fingerprinting dates back hundreds of years.

Fingerprinting with ink and paper was common in the past. However, through the advances of technology, electronic forms are now common. There are many different types of devices for capturing fingerprints electronically. These include optical readers, thermal imaging, and electromagnetic field imaging (Meenen & Adhami, 2001) as well as capacitance testing and ultrasound (Bolle, Connell et al., 2004). Each has their own individual characteristics (beyond the scope of this paper). But, for the most part, once they are captured, the basis for identification is similar.

Precise Biometrics SC-100

Sony FIU-710

Bioscrypt Veriprox
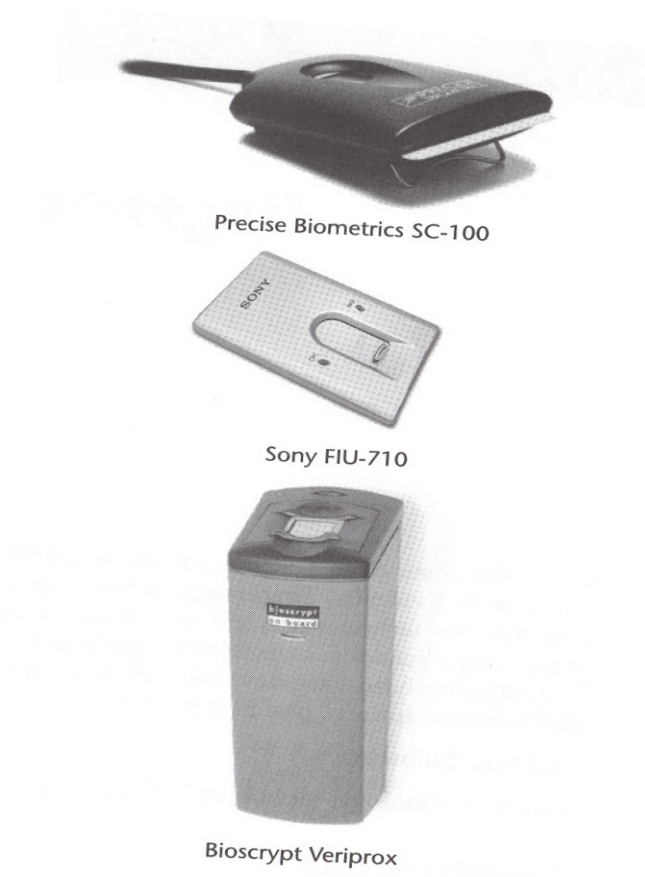
Figure 7: Example of Print Capturing Devices
(Nanavati, Thieme et al., 2002)

Fingerprinting systems attempt to capture the ridges and valleys of the fingerprint. These ridges and valleys form distinctive characteristics called minutiae. Minutiae can be classified as either ridge endings or bifurcations (Nanavati, Thieme et al., 2002). Figure 8 below details the difference.

a: ridge ending
b: bifurcation
c: independent ridge
d: ambiguous ridge ending / bifurcation
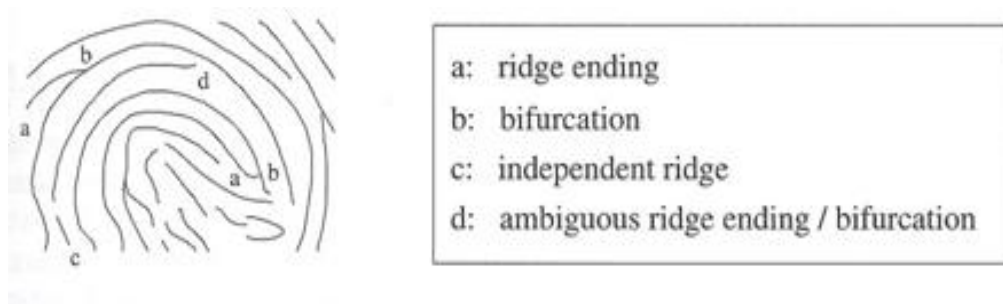
Figure 8: Basic Example of Minutiae
(Bolle, Connell et al., 2004)

It is these unique identifiers that are extracted and captured and recorded for future comparison. This technology accounts for 80% of the fingerprinting methods today. In other cases, pattern matching, based on the ridges, is used (Nanavati, Thieme et al., 2002).

Hand Geometry

Hand geometry identification and verification is based on the idea that the geometric structure of the hand can be used as a unique identifier. While not measuring on quite as fine a scale as fingerprints, hand geometry is distinguishing enough to employ for some verification needs (Woodward, Orlans et al., 2003). Hand geometry measures characteristics of the hand such as length, thickness, finger size, overall surface area, and width. For this technology to be effective, the user must present his or her hand to a

reader, where a mirror reflected image is captured via a camera. In most cases, guides

exist to help the user align their hand to a predetermined position. This helps to minimize

variations in the image capture (Woodward, Orlans et al., 2003). Figure 9 below depicts

a typical hand geometry device and image.
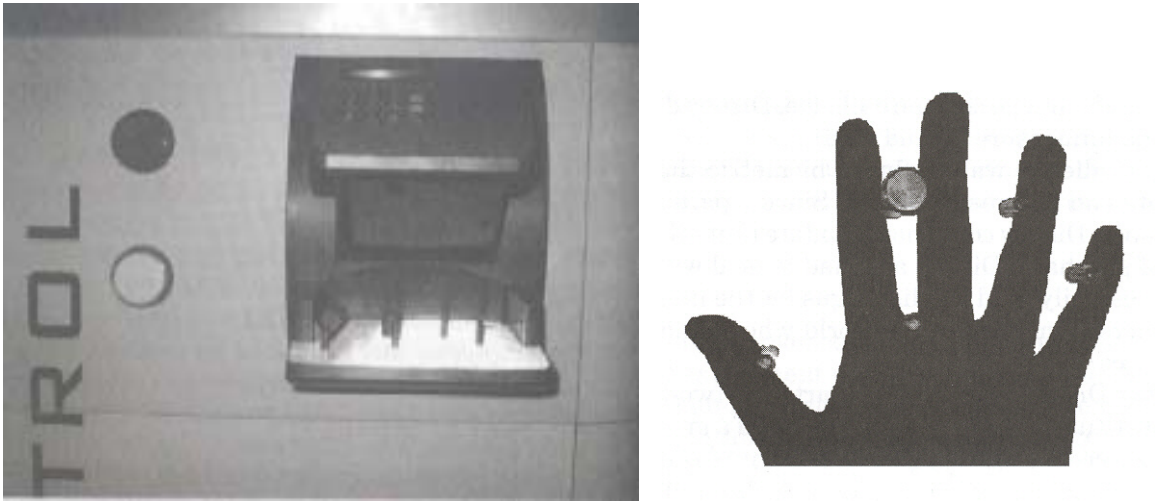
Figure 9: Hand Geometry Reader & Capture
(Woodward, Orlans et al., 2003)

The following sections will look at a couple of techniques dealing with the human

eye. Specifically, these will include iris scanning and retinal scanning. Figure 10 below,

details the components of the human eye. Particular attention should be paid to the

location of the iris and the vessels at the back of the eye where the retina scan takes place.
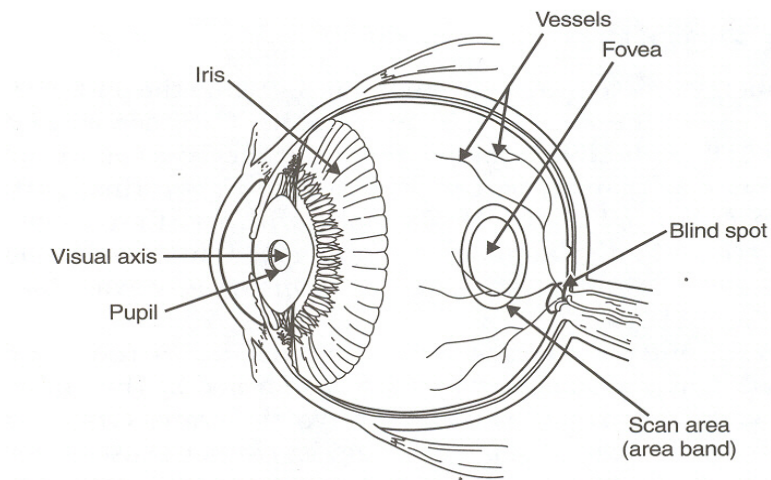
Figure 10: Detail of the Human Eye

(Woodward, Orlans et al., 2003)

Iris Scan

To be effective, the technology of the iris scan depends on the unique features of the iris. The iris is the colored portion of the eye that controls the size of the pupil and further, the amount of light let into the eye. This technology, again, requires a camera as the capturing device in addition to an infrared imaging unit (Nanavati, Thieme et al., 2002). The user need only to look into the system, the image of the iris is captured and then a template is created and processed.
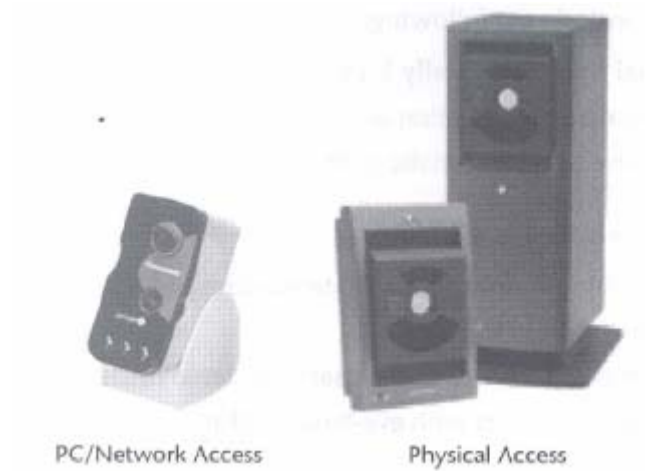
Figure 11: Iris Scan devices
(Nanavati, Thieme et al., 2002)

Depending on the manufacturer and model type, users may need to be as close as a few inches to the hardware unit or can be as far away as a few feet (Nanavati, Thieme et al., 2002). The image taken is encoded using a circular grid as its guide and patterns are collected, and then converted to a bar-code system as indicated in Figure 12. It is this barcode that is stored as the template for future identification or verification (Negin, Chmielewski et al., 2000).
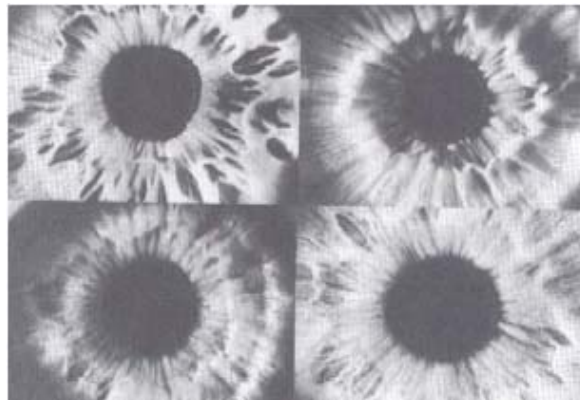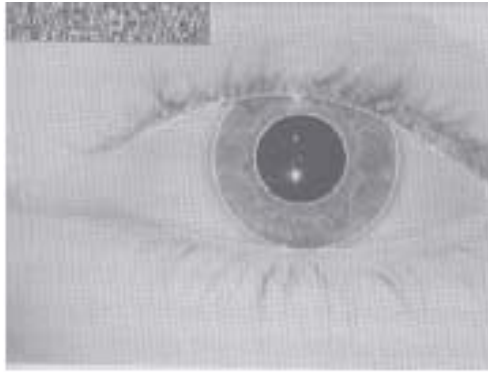
Figure 12: A Typical Iris Image and a Coded Scan
(Nanavati, Thieme et al., 2002)

Retina Scan

A retina scan, while sounding quite similar to iris scan, is in fact much different.

The retina is that portion on the back, inside surface of the eye (reference figure 10).

Retinal scanning, as a biometric, uses the patterns of veins in this area of the eye to

determine individuality. The user is required to stare into the capturing device. Next, the

area is illuminated with an infrared light and a pattern image of the major blood vessels is

attained (Woodward, Orlans et al., 2003). As with other systems, this image is then

compared to one on file for verification or identification. The user in this case is required

to be in very close proximity (2-3 inches) to the capture device. Additionally, as with the

other biometrics discussed thus far, the retina is considered to be a unique identifier and,

barring traumatic injury, a stable and relatively secure one at that. The retinal patterns

cannot be changed without willful alteration or disfigurement (Woodward, Orlans et al.,
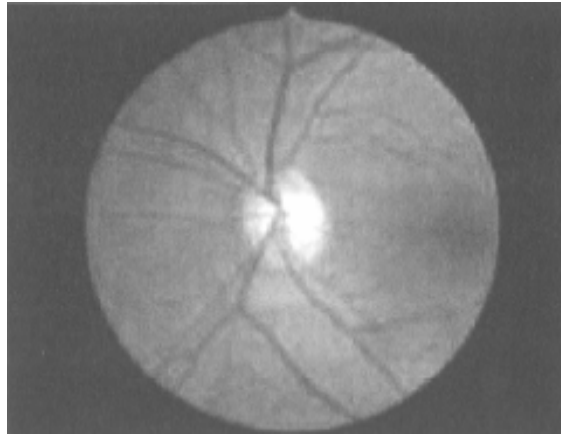
2003)

Figure 13: A Human Retina Scan

(Woodward, Orlans et al., 2003)

Facial Recognition

Facial recognition systems are gaining momentum as of late. The reason for this is that facial recognition systems are non-intrusive. Because of facial recognition's non – intrusive nature, a person's face can be scanned from a discrete distance. Couple this with the fact that the image can be captured without the individual's consent or knowledge and it is easy to understand why this technology is getting so much attention. Additionally, monitoring technology is present in our everyday life. From the convenience store and bank surveillance systems to the traffic camera on the street corner, video technology is everywhere.

There are a couple of different methods currently being used for facial recognition. Mostly, these technologies rely on the distinct features of the face, such as location of the eyes, nose, lips, and the relationship between these parts (Jain, Hong et al., 2000). One method, face geometry, focuses on the position or layout of the features and a feature constellation for comparison (Bolle, Connell et al., 2004). Another method, based

30

on face appearance, captures the distinctive characteristics of the face without capturing the entire image, reducing it to a smaller pixel quantity (Bolle, Connell et al., 2004).
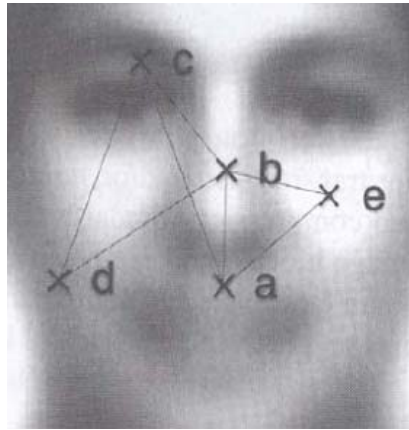
Figure 14: Facial Scan
(Bolle, Connell et al., 2004)

While this technology is relatively young, it shows some distinct promise for the future.

Voice Recognition

Voice recognition is a technology that captures the vocal quality of the human voice. Characteristics such as pitch, inflection, intensity, and some that can't be heard by the human ear, can be captured (Nanavati, Thieme et al., 2002).The voice signal is first converted from analog to digital format, the key portions are extracted, and then sent to the authentication system for verification or identification. As with other methods of biometrics, the enrollment process is critical to voice recognition systems. Speech recognition can be broken into the following categories (Bolle, Connell et al., 2004):

- Fixed Test: Requires the speaker to pronounce a prearranged phrase or selection of words.

- Text Dependent: For authentication, the speaker must say a specific word or phrase.

- Text Independent: the speaker can say anything he or she wants to say. There is not a set pattern for recognition to take place.

- Conversational: Speech is recognized and the user is verified through the process of conversation. But, this is not the only component. Additionally, secret knowledge is required and acquired via this conversation. (Bolle, Connell et al., 2004)
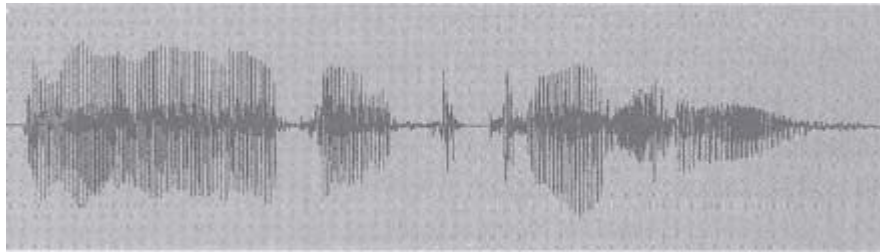
Figure 15: A Captured Voice Print
(Bolle, Connell et al., 2004)

Voice recognition is very popular because it is a low cost option that can take advantage of mature technology.

Signature Recognition

Signature recognition is the ability of a system to recognize a user's signature. This technology goes beyond mere verification of the shape of a signature. Some systems are able to differentiate between pressure, acceleration, and velocity of the

signature being written (Jain, Hong et al., 2000). Interestingly, these characteristics are very difficult to mime or mimic making the signature verification biometric very desirable (Nanavati, Thieme et al., 2002). Consider the implications in the financial community alone where a signature is already an accepted form of personal identification (Jain, Hong et al., 2000).

Other Forms of Biometrics

There are additional forms of biometric technology making their way into the mainstream. Technological advances allow the practical development and implementation of these newer forms. Each shows potential as a viable solution to some of our most difficult identification and verification problems. These technologies have already shown much promise and could certainly play, or continue to play, a large part of our future.

- DNA – Short for Deoxyribonucleic Acid, DNA has become one of the more common forms used by law enforcement officials. DNA carries our genetic makeup and has become widely respected and accepted throughout the world. However, the extraction and use of DNA as an authenticator is difficult and requires time. As such, it currently cannot be considered an automatic method of authentication (Ortega-Garcia, Bigun et al., 2004).
- Keystroke Scan – This is an attempt to capture distinctive patterns in the way a person types on a keyboard. The measure of time between strokes, the use of the keys, hold patterns, etc. This is a behavioral biometric (Nanavati, Thieme et al., 2002). A plus for keystroke scanning is that it uses existing hardware.

- Ear Shape – The shape of the human ear is a characteristic that has begun to get some attention. Although not yet widely accepted, this field is again based on the premise that the ear is a unique feature that can be analyzed and used as a form of identification.

- Gait – This is the measurement of the distinctiveness of a person's walk (Woodward, Orlans et al., 2003). The person's body motion, or body language, is used and translated into a language that a computer can understand. This biometric is based not only on motion, size, build, and the like, but emotional state, environment, etc (Woodward, Orlans et al., 2003).

- Body Odor – The chemical makeup of an individual lends itself to a unique body odor. Dogs have been used for long periods of time to track human beings. Research to create a device (an electric "nose" with chemical receptors (Woodward, Orlans et al., 2003)) to track chemical compositions, or chemical scents, is already well underway and making progress.

A variety of technologies exist in the biometric field. This table, created by Blackburn, et al. (2003), shows a side by side comparison of typical characteristics of those technologies already introduced. These characteristics, while not addressing all areas of concern, do present a good picture of the overall diversity, effectiveness, and problem areas often associated with these technologies.

Table 1: A Comparison of Selected Technologies
Source: (Blackburn, Butavicius et al., 2002:vi)

Biometric	Finger	Face	Hand	Iris	Retina	Voice	Signature	Keystroke	Ear	DNA
Access control	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Surveillance	N	Y	N	N	N	Y	N	N	Y?	N
Accuracy	very high	high	high	very high	very high	med	med	low	?	very high
Reliability	high	med	med	high	high	low	low	low	low	high
Error rate	1 in 500+	no data	1 in 500	1 in 131,000	1 in 10 mil	1 in 50	1 in 50	no data	?	no data
Errors	dryness, dirt, age	light, age, glasses, hair	hand injury, age	poor light, contact	glasses, contact lenses	noise, cold weather	alter style	hand injury, tired	light, hair	none
False positives	highly unlikely	unlikely	very unlikely	very unlikely	highly unlikely	likely	likely	unlikely	?	highly unlikely
False negatives	highly unlikely	very likely	likely	very unlikely	highly unlikely	very likely	very likely	very likely	?	highly unlikely
Security	high	med	med	high	high	med	med	med	?	high
Stability	high	med	med	high	high	med	med	low	?	high
User acceptance	med	med	med	med	med	high	high	high	?	low
Intrusiveness	med	low	low	low	very high	low	low	low	low	high
Ease of use	high	med	high	med	med	high	high	high	med	low
Low cost	Y	Y	N	N	N	Y	Y	Y	Y	N
Standards	Y	?	?	?	?	?	?	?	?	Y
Strengths	existing databases in operation	surveillance, checkable by humans, can use existing equipment		high accuracy	accuracy	low cost, can be used for surveillance	low cost	low cost, no additional hardware required	profile imaging possible, surveillance use	accuracy
Weaknesses	public acceptance, environment-ally affected, specialised hardware	environment-ally affected, biometric changes	environment-ally affected, biometric changes, specialised hardware	public acceptance, glasses, specialised hardware	public acceptance, glasses, specialised hardware				environ-mentally affected	not real-time, expensive, specialised operations, specialised hardware

The Case for Biometrics

To make a case for the use of biometrics, it is important to examine what positive characteristics biometric technology brings to the identification and authentication realm.

First and foremost, it is essential to realize that current methods of authentication, outside the realm of biometrics, just cannot meet all demands alone. Personal identification numbers (PIN) can't handle the job anymore (McHale, 2003). Ratha et al. (2001) explain that, "…traditional authentication policy based on a simple combination of user ID and password has become inadequate." (Ratha, Connell et al., 2001:615) They go on to say that password systems are more susceptible to brute force attacks, for example, than a biometric system is because of the effort it would take to crack a biometric system (Ratha, Connell et al., 2001:615). Traditional password methods have other limitations as well. Password and PINs can be easily forgotten or guessed (Ribaric, Ribaric et al., 2003). Often, users will employ the same password across multiple systems potentially opening many doors should their password become compromised (Uludag, Pankanti et al., 2004). Consider too, some users will write down passwords further increasing the chances of compromise (Uludag, Pankanti et al., 2004).

Next, traditional methods of authentication, such as user ID and password, as well as token based methods, are only useful for positive recognition applications, not negative (Jain, Ross et al., 2004). With the employment of a biometric system, negative recognition is possible and can prevent a single user from using different identities (Jain, Ross et al., 2004).

36

Subsequently, biometric identifiers possess some unique traits that other forms of authentication do not provide. As a form of identification and authentication, biometrics:

- Cannot be lost or forgotten (Matyas & Riha, 2003; O'Gorman, 2003; Seno, Sadakane et al., 2003; Uludag, Pankanti et al., 2004; Woodward, 1997).

- Provide user convenience, user no longer need to remember several passwords or the long and complex ones needed for enhanced security (Prabhakar, Pankanti et al., 2003; Seno, Sadakane et al., 2003).

- Are extremely difficult to copy or share (Ratha, Connell et al., 2001; Uludag, Pankanti et al., 2004).

- Are difficult to forge and more costly to try and crack than passwords (Prabhakar, Pankanti et al., 2003; Uludag, Pankanti et al., 2004).

- Are relatively equal between users. In other words, no one user's biometric is easier to manipulate than the next (Uludag, Pankanti et al., 2004).

- Provide a degree of non-repudiation. It is unlikely that a user who has accessed some form of media will be able to repudiate having accessed it if biometrics have been used (Prabhakar, Pankanti et al., 2003; Uludag, Pankanti et al., 2004). Passwords and PINS can be dishonestly acquired by covert surveillance and when this happens, there is no protection against repudiation by the authorized owner (Ratha, Connell et al., 2001). Also, biometrics profess to inextricably tie the authenticator to its owner providing non-repudiation (O'Gorman, 2003).

- Could possibly increase the user's perception of accountability for their actions (Rejman-Greene, 2001).

- Enhances security. Used in conjunction with other methods, such as user ID and password, a smart card application, the use of biometrics provides an additional layer of security (Liu & Silverman, 2001; O'Gorman, 2003).

The large number of advantages presented illuminates the general capabilities of several of biometric technologies. But, to be of use, we must anticipate the bad with the good. Therefore, the next section will identify a few areas of the biometric field that tend to be looked at as areas of concern and issues that must be addressed.

Biometrics: Issues and Concerns

While experts agree that biometric technologies show much promise and provide a great number of advantages, it is important to recognize that a growing list of concerns is present as well. As a precursor to any implementation, these concerns should also be thoroughly investigated and considered. Issues that must be addressed include:

- No single biometric can effectively meet the challenges of all applications (Jain, Ross et al., 2004; Prabhakar, Pankanti et al., 2003). No one technology is the perfect biometric (Jain, Ross et al., 2004; Woodward, 1997) and each technology presents its own unique challenges.

- Biometric samples provide uniqueness but not secrecy (Jain & Uludag, 2003). For example, we leave fingerprints everywhere we go and our facial image can be captured without knowledge (Jain & Uludag, 2003).

- Each biometric technology has strengths and weaknesses (Jain, Ross et al., 2004; Prabhakar, Pankanti et al., 2003) that must be evaluated before use or implementation.

- A compromised biometric feature is compromised forever (Prabhakar, Pankanti et al., 2003). As an example, we only have one face or two retinas. In user ID/password and token systems, a compromise can more easily be avoided by changing passwords or canceling the token (Ratha, Connell et al., 2001).

- Privacy issues abound. Digital formats of unique biometrics could possibly be shared between federal or commercial enterprises without the owners knowledge or consent (Ratha, Connell et al., 2001). Also, many consider the presentation of a biometric a lose of anonymity and autonomy (Matyas & Riha, 2003; Woodward, 1997).

- Identity theft has been considered an issue as well (Dunstone, 2001).

- Some users may consider biometrics authentication techniques to be invasive and may not accept them (Matyas & Riha, 2003; Ortega-Garcia, Bigun et al., 2004). Generally, the less intrusive the biometric, the more willingly it will be received (Liu & Silverman, 2001).

- Some technologies are difficult to use and are not considered user friendly (Liu & Silverman, 2001).

- System errors can be an issue. As discussed earlier, a tradeoff exists between accuracy and security. FAR, FRR, FTE, and must be considered individually for each implementation.

- A biometric characteristic's greatest strength, its invariability over time, is also one of its greatest flaws (O'Gorman, 2003; Ratha, Connell et al., 2001).

- As with all systems, cost is a concern. Unlike a traditional password system, biometric systems, as with some token systems, generally require specialized

39

hardware. This relates to increased costs and in some instances could be

prohibitively high for smaller organizations (Dunstone, 2001).

- Biometric systems, like all systems, are susceptible to attack. These

    vulnerabilities include the presentation of fake samples, tampering with templates,

    or attacking any portion of the system that processes necessary components

    (Ratha, Connell et al., 2001)

- Standards agreement is slow to develop on a national or global scale.

The previous section detailed some of the problems associated with the use of biometric

technologies. Those issues and concerns detailed must be considered within the overall

scope of use. While we welcome the advantages of using biometrics, we must be sure to

reflect on the fact that with those advantages come associated costs.

Summary

The chapter provided a comprehensive look at the DOD IA model and the five

keys components of authentication, non-repudiation, availability, integrity, and

confidentiality critical to a DOD IA effort. Next, the science of biometrics was explained,

common technologies were detailed, and data explaining the potential and promise of

these technologies were presented. Additionally, areas of issue and concern were also

presented. The next chapter, Chapter III, will detail the research methodology specific to

this study.

III. Methodology

Chapter Overview

The purpose of this chapter is to introduce the technique and rationale for the methodology used in this research effort. This chapter will lay the foundational framework for using the historical research method and justify its use for the research being conducted.

The Historical Research Methodology

Much can be learned from the study of history. Historiography, as described by O'Brien et al (2004) is:

> "… an empirical research paradigm using an interpretative or qualitative approach which focuses on a chronology over a substantial period of time in order to obtain a fuller and richer understanding of a situation or set of circumstances." (O'Brien, Remenyi et al., 2004:137)

Leedy and Ormrod contest that the heart of the historical method is not the accumulation of facts but rather the interpretation of the facts (Leedy & Ormrod, 2001). This seems like a rather simplistic view but it allows us to differentiate between the historical method and the study of history. Rather than just gathering significant facts about an event and organizing them, the historical researcher will try to synthesize events into meaningful clusters (Leedy & Ormrod, 2001). Furthermore, Mason, et al (1997b) believe that,

> "The final outcome of an historical study, consequently, is an account: a comprehensive story, a complete episode that has a beginning, a middle, and an end. As the account unfolds, it illuminates the events, forces, and personalities that brought about the circumstances, detailed by the facts." (Mason, McKenney et al., 1997b:315)

While it may seem like only historians would use this method, disciplines such as

geography, history, literature, and others can make use of it as well (Leedy & Ormrod,

2001). In fact, the application of the historical method can be, and has been, applied to

management information systems (MIS) as well (Mason, McKenney et al., 1997a).

Mason et al (1197b) tell us that this methodology plays an important role:

> "Histories of the use of information technology in business will provide
> modern day leaders with new insights into the managerial and economic
> processes at work in this new era and how to employ them effectively and
> responsibly." (Mason, McKenney et al., 1997b:318)

It is important to address the applicability of the historical research method to

information systems for this research effort. Because the use of technology plays a large

part, it is important be able to tie this effort to a research framework. This can be

accomplished through several important works.

An approach has been developed to address an historical research method as

related to Management Information Systems (MIS) by Mason, McKenney and Copeland

(1997). This approach, called the Cascade, lays a foundational structure for IS and was

developed in an effort to explain the materialization of information systems in the work

environment. This 5 step framework is based on the assumption that a crisis must exist

before IS will be used. Once the crisis is identified, the following steps are followed:

1. There is a search for a technical solution.

2. An initial technical solution is found.

3. Adjustments are made throughout the organization.

4. Assets are formed, which resolve the crisis.

5. Dominant Design is achieved

The end stage, dominant design, can be explained as finding and putting together the right combination of company resources (people, strategies, operations, customers, suppliers, etc.) to achieve superior results and innovation. (Mason, McKenney et al., 1997a).   This forces competitors to respond in order to keep up (Mason, McKenney et al., 1997a).

Bannister (2002) however, disagrees with the idea that a crisis must exist and that dominant design must be achieved in order to learn. In fact, there is still much to learn from historical studies of organizations that don't face a major crisis or have not achieved a dominant design (Bannister, 2002).

Applying Mason's historical method specifically to the MIS field, the cascade framework of information systems is facilitated by a seven step method. Mason et al (1997b) define the seven steps as:

1. *Begin with focusing questions* – create focus questions on the area of inquiry.

2. *Specify the domain* – the range of events must be determined.

3. *Gather evidence* – collect data for historical interpretation and develop the researcher's tacit understanding and intuition of the phenomena under study.

4. *Critique the evidence* – evaluate the evidence for applicability and relevance.

5. *Determine patterns* – interpret the facts and comprehend their meaning.

6. *Tell the story* – write the narrative while maintaining the integrity and consistency of the evidence.

7.   *Write the transcript* – place the historians words in context with the existing

schema (Mason, McKenney et al., 1997b).

While the Cascade method is used to evaluate information systems and is not specifically

used in this effort, the seven step process used to facilitate that method can be applied to

the research effort at hand.

In yet another effort to define historiographic research, O'Brien et al. (2004)

developed a nine step framework similar to Mason's outlined above. While geared

toward business and management studies, this framework has many similarities. The nine

steps as outlined by O'Brien et al (2004) are:

1.   *The research question* – research must have a focused research question,

must be defendable, and have a chronological importance.

2.   *The relevance check* – the researcher must be sure an historical analysis

would be useful.

3.   *The scope of the research* - establish the domain/scope of the research effort.

4.   *Sources of evidence* – collect evidence from credible primary and secondary

sources.

5.   *Assessment of methods of analysis* – the researcher must determine whether

a qualitative, quantitative, or a hybrid approach to analysis will be used.

6.   *Assembling* the evidence – evaluate and construct the support for the

research.

7.   *Developing the story* – the researcher must determine the patterns present,

address the issues of what, how, and why and then tell the story.

8.   *Critiquing the story* – the researcher must apply critical analysis skills to
    determine whether or not the evidence presents a compelling argument.

9.   *The outcome of the research* – express the findings of the research and
    explain what the research effort contributed to the existing body of
    knowledge.

Table 2 below shows a side-by-side comparison of the two methodologies and

demonstrates where the researcher believes similarities exist.

Table 2: Historical Methodology Comparison
(O'Brien, et al. (2004) and Mason, et al. (1997b))

O'Brien's 9 step methodology for Business & Management Studies(2004)	Mason's 7 step methodology for MIS (1997b)
1. The research question	1. Begin with focusing questions
2. Relevance check	
3. Scope of the research	2. Specify the domain
4. Sources of evidence	3. Gather evidence
5. Assessment of methods of analysis	4. Critique the evidence
6. Assembling the evidence	
7. Developing the story	5. Determine patterns
8. Critiquing the story	6. Tell the story
9. The outcome of the research	7. Write the transcript

Both of these frameworks provide a foundation upon which to answer the investigative

questions and research question. All questions will be explored, studied, and evaluated in

the context of the research objective. However, for the purpose of this research effort, the methodology defined by Mason (1997) will be used.

Justification for the Historical Research Methodology

Historical analysis provides a unique perspective from which to see things. Knowing the background of a situation or to any issue enhances our comprehension and improves our ability to see what is important and what is not (O'Brien, Remenyi et al., 2004). Additionally, as McDowell (2002) states,

> "It is the discipline of history which provides us with the opportunity to understand and appreciate the past, to distinguish myth from reality, and to see which elements of the past had an influence on future events." (McDowell, 2002:3)

Although a relatively recent development in the world of information systems, historical research and development plays an important role. According to Mason et al., historical analysis broadens our understanding of the processes by which information technology is introduced into organizations and the forces that shape its use (Mason, McKenney et al., 1997a). Additionally, Mason et al (1997b) tell us, the use of an historical research methodology in IS provides three valuable products:

1. An account of a significant fragment of the past describing events of importance to the MIS community. The account in and of itself is informative, but it also serves as contextual material for understanding other events (Mason, McKenney et al., 1997b).

2. The resulting historical account may be used subsequently as a "datum" in a broad process of inductive reasoning (Mason, McKenney et al., 1997b).

3. Historical research may serve as the source of new research hypotheses (Mason, McKenney et al., 1997b).

In addition to these three, Bannister (2002) contends that another important result comes about: validation and falsification of existing theory (Bannister, 2002).

Validity

In order for this research effort to produce convincing results, it is important to address the validity of the data being used. Leedy and Ormrod (2001) suggest that historical data are subject to two types of evaluation: authenticity and meaning, also called external evidence and internal evidence respectively (Leedy & Ormrod, 2001). To explain further, the data must first be evaluated as coming from a genuine source. This is authenticity. Next, if the document or data is determined to be authentic, it must then undergo further scrutiny to determine its value and meaning to the research being conducted (Leedy & Ormrod, 2001).

Limitations

It is important to note several limitations when using the historical method for research. First, any research effort, researcher bias can affect the research (Leedy & Ormrod, 2001). While careful attention is paid to eliminate as much of this bias as possible, it is impossible to eliminate it completely. Each researcher will have arrived at their research effort via different paths, with different experiences. These influences will certainly affect the researcher's efforts. Consider, too, the fact that each researcher will have their own criteria for accepting or rejecting evidence (O'Brien, Remenyi et al., 2004). What may be a perfectly acceptable source to one researcher may not be to

another. For the purpose of this research, the author assumed all included references met the first criteria of being authentic. To the largest degree possible, material was considered to come from professional, peer reviewed, credible journals and publications as well as original DOD documents in their most current form.

Next, Mason et al (1997b) point out that some of the researcher's assumptions in any historical study gets mirrored back during the study. Again, while the researcher attempts to eliminate as much of this as possible, it is impossible to eliminate it all. After all, researchers will always have preconceived notions prior to the study. The researcher's a priori beliefs will manage to creep their way in to the research effort (Mason, McKenney et al., 1997b).

Also, because the researcher is studying facts and data from the past, they can be difficult to understand. The researcher will have to interpret data from events he or she was most likely not in attendance for (Bannister, 2002). This can be compounded by the notion that the historiographer is more than likely not working from a complete set of information (O'Brien, Remenyi et al., 2004).

Finally, because the historical research framework is qualitative in nature, it lacks mathematical tractability (Mason, McKenney et al., 1997b). In fact, qualitative research, because of its subjective nature, was slow to gain acceptance as legitimate research but has since gained widespread recognition (Leedy & Ormrod, 2001).

Summary

This chapter described the historical research methodology. It outlined the basic methodology and detailed the methodological framework as it pertains to information

systems and to business and management studies. It also explained how these foundational concepts were applied to both the research question and the investigative questions previously discussed. Finally, the historical research methodology was used as an investigative tool to address and answer the investigative questions and overarching research question. The next chapter, Chapter IV, will contain an analysis of the literature reviewed and how it relates to the research effort. In addition, the investigative questions and the research question will be addressed.

<center>**IV. Analysis and Results**</center>

Chapter Overview

   The previous chapter explored literature related to the DOD IA framework and

biometric technology. This chapter will discuss how that literature relates to and answers

the investigative questions as well as the research question proposed earlier in Chapter I.

Questions Answered

  Investigative Question One

   The first investigative question asks, "What components are considered

critical to the DOD IA model?" Through careful review of the available DOD literature,

five key components have been identified as essential to a robust IA model. According to

JP 3-13 (1998) those key elements are:

> ➢ Authentication – the ability to be able to verify the originator.
>
> ➢ Non-repudiation – irrefutable proof of participation.
>
> ➢ Availability – assured access from unauthorized users.
>
> ➢ Confidentiality – protection from unauthorized disclosure.
>
> ➢ Integrity – protection from unauthorized change.

These five pieces address key components of security. By focusing our efforts on

addressing these areas, we can hope to effectively build a comprehensive IA program

robust enough to protect even the most sensitive of our assets.

   Additionally, literature external to the DOD also pointed to these five components

as being integral to a comprehensive IA program. This literature reinforces the idea that

the DOD model and its five components are robust enough to address the IA concerns of the DOD.

Investigative Question Two

Investigative question #2 asks, "What advantages do biometric technologies provide that may contribute positively to IA efforts?" A thorough review of the literature suggests that in a broad sense, biometric technologies provide a great many advantages. Multiple experts have touted the ability of biometrics to alleviate common password management problems. Where other forms of authentication have fallen short and seem to be inadequate, biometrics seem to shine. They provide a larger degree of security over password or token based measures. Biometric technologies provide an answer to the forgotten, written down, or shared password vulnerabilities as well as the lost token difficulties. Biometrics are more convenient to use than remembering multiple passwords and provide a level of non-repudiation that password and token based measures forego.

Subsequently, the literature also suggests that biometric technology is robust and increases security. Multiple authors point specifically to the fact that biometrics are difficult to forge or copy and would be costly to crack. This compounds the effects of those mentioned in the previous paragraph. Clearly, the advantages to using biometrics are worthy of the time and effort necessary to properly integrate them into our information systems infrastructures.

Investigative Question Three

Investigative question #3 asks, "What concerns have been raised regarding the use of biometric technologies that may hinder IA efforts?" Here, again, the literature is clear.

51

While the advantages of using biometric technologies are evident, issues and concerns with the technology abound as well.

First and foremost, the literature reviewed clearly suggests that no single technology can address all verification and identification problems or concerns. Rather, each technology has areas where it might be more suitable than another. With each come inherent difficulties. These difficulties cannot and should not be overlooked. Furthermore, in most cases, a trade off exists between security and usability. The more secure a system needs to be, the higher the price to be paid. This price may not necessarily equate to tangible figures. For example, the increased cost may liken to decreased usability for the user. Additionally, the more difficult a system is for the users, the less likely they are to be satisfied with it.

Next, privacy issues are at the forefront of many experts' minds. The use of biometrics opens the flood gates to privacy concerns. The literature suggests multiple areas to be apprehensive about. Sharing of personal data, compromise of unique characteristics and loss on anonymity and autonomy are all on the list. Additionally, areas of unease include the escalating arena of identity theft. As pointed out in the literature, once a biometric trait is compromised, it is compromised forever and cannot be "reset" like a password or replaced like a token.

Finally, tangible costs are a concern. The use of biometrics will invariably involve an increase in material costs. Because this technology requires, in most cases, unique hardware, costs to implement and maintain will be incurred.

Investigative Question Four

Investigative question #4 asks, "Which components of the IA model can be addressed by the use of biometric technologies?" As the literature revealed, the use of biometric technology can address several aspects of the DOD model.

First and foremost, the issue of authentication can be addressed. Biometrics can be used as authentication technologies. The use of these technologies fortifies this portion of the model by providing stronger methods of authentication. They address the shortcoming of two traditional means of authentication, knowledge based and token based, and provide for alternate means of verification and identification.

Next, the concept of non-repudiation is strengthened by the use of biometrics. Unlike other methods of authentication, biometrics can conclusively provide a measure of non-repudiation. Other methods fall short in this area. Depending on the implementation of the biometric technology, non-repudiation is attainable because of the security of biometrics. As the literature indicated, it is extremely difficult to forge or steal a biometric attribute. In other authentication schemes, a username and password or a token might be stolen or lost. In these cases, there is no undeniable way to tell that participation in a transaction had taken place by someone other than the intended participant. The use of biometrics solves this problem. The strengths of these technologies and the amount of non-repudiation they provide can nearly alleviate these concerns.

The component of confidentiality can be addressed with biometrics as well. Here, biometric technologies offer a more robust authentication method that is less likely to be compromised. Because of this, maintaining the confidentiality of our systems and the information they contain is simplified. Through the use of a properly employed biometric

technology as an authentication method, we insure that we disclose information only to the intended parties and avoid compromise.

Finally, the component of integrity can be enhanced by the use of biometrics. By providing an environment in which access is strictly controlled with a robust authentication system, we can hope to ensure that information remains free from corruption or unauthorized change. While the case for biometrics is tied to their ability to act as a robust authentication system, the fact remains that the IA component of integrity can be enhanced by the presence and use of these technologies on our systems. This directly enhances our IA efforts.

Research Question

The main research question for this effort is, "In what manner, if any, does the use of biometric technology act as an enabler to information assurance?" This question can be answered by synthesizing the answers to the four investigative questions but most specifically, by investigative question four.

Biometric technology acts as an enabler to information assurance by providing a means to address critical components of the information assurance model. The use of biometrics as a means of verification and identification provides the tools necessary to achieve four essential components to the DOD IA model, specifically authentication, non-repudiation, confidentiality, and integrity. With this in mind, it will be important to effectively evaluate other areas of the field of biometrics. This will be necessary to ensure that not only are we employing the proper technologies, but that we are employing them in the right situations and with the right expectations of their performance as well.

Arbitrarily employing these technologies in an effort to streamline or enhance the DOD

IA efforts is not what is needed. Rather, careful evaluation, consideration, and

implementation will allow the use of biometric technology to enhance and further support

the information assurance efforts of the DOD. Continued research in all areas will pay

dividends by complementing ongoing efforts in both fields of endeavor.

Summary

This research effort focused on binding the scientific field of biometrics to the IA

model used within the DOD. Through the use of an historical analysis, the author

attempted to synthesize facts, ideas, and thoughts of multiple expert sources to determine

the significance of the contribution biometric technology makes to the DOD IA model.

The next chapter, Chapter V, will summarize the conclusions of this research as well as

present some recommendations for future research.

V. Conclusions and Recommendations

Chapter Overview

The final chapter of the research effort will begin with a conclusion of the overall research effort and the significance of this research effort. It will then conclude with some recommendations for future research and a summary.

Conclusions of Research

This research focused on binding the scientific field of biometrics to the IA framework used within the DOD. Through the use of an historical analysis, the author attempted to synthesize facts, ideas, and thoughts from multiple expert sources and interpret them within the context of both fields of study.

Additionally, this research effort provides enough evidence to suggest that the use of biometric technology *is* an enabler to the overall IA effort being pursued by the DOD. By positively influencing four of the five components of the DOD IA model, the use of biometrics significantly contributes to the overarching goal of IA.

However, it is important to note that with all the positive benefits these technologies bring to bear, they also bring with them issues that must be addressed. Here, we must be diligent enough to evaluate the specifics of each technology and address both the positive and negative qualities of each.

Significance of Research

This research effort provides several significant conclusions. First, the use of biometric technology can greatly enhance any overall authentication effort. Properly

implemented, biometric technologies used in authentication systems provide a more robust scheme for identifying and authenticating users. The literature is clear in this area. Next, this research suggests that biometric technology is a tool that should be used as an enabler to the IA efforts of the DOD. With the need for robust IA on the rise, it will be important to employ technologies such as biometrics to help combat the threats that exist and those yet to come. Finally, this research conclusively ties biometrics to the IA model and lays the foundation for further investigation and research.

Recommendations for Future Research

As mentioned earlier, through the use of an historical analysis, this research effort focused on binding the scientific field of biometrics to the IA framework used within the DOD. However, it is important to note that additional research should be undertaken in an effort to move forward. With the depth of the field of biometrics, many areas are open to exploration and this future research will be necessary to further DOD efforts with these technologies. While this research effort focused on establishing a connection between the two fields of endeavor,

For example, it might be valuable to conduct a Delphi study of DOD experts or their civilian counterparts to determine the perceived usefulness and impact of biometric technology on their respective areas of influence. Key concepts to investigate and evaluate could include the overall usefulness of biometric technology, and the effect biometric technologies have had on specific areas of information assurance and security. In addition, this expert opinion could provide some additional insight into additional use or implementation issues.

Next, individual technologies, retinal scan for instance, could perhaps be further evaluated via case study research in an effort to determine user acceptance of them. While some forms of biometrics are not considered to be intrusive, others can be considered quite invasive. Quite possibly, an evaluation of these in the context of an existing technology acceptance model (Davis, 1989; Davis, Bagozzi et al., 1989), could be beneficial by providing additional insight.

Additionally, further research could evaluate the technologies themselves in the context of the DOD environment. As indicated in the literature review, not all technologies are appropriate in all situations. The unique requirements of the DOD environment may further complicate this issue. Case study research to evaluate actual implementations may provide additional insight into the unique needs of the DOD and its security concerns.

Finally, there are numerous areas linked to the field of biometrics that were not fully addressed in this study. Legal issues, privacy, standardization of systems, accuracy of systems, testing and evaluation, and cost related issues, are all areas of study that could benefit from additional research.

Summary

The use of computers and technology will continue to grow in the future. As more and more people around the world get connected, the threats to our systems grow. The field of information assurance is a defense that we must be sure to have in place. Enablers to that defense are critical.

There is no question that the science of biometrics is gaining ground and will be a widespread reality in the near future. While the use of biometrics is certainly promising, their use alone is not a magic cure-all to the identification and verification woes of today's complex, technology ridden environment. A panacea just does not exist. Evaluated smartly and used properly, in conjunction with other proven methods, biometric technology is sure to add a level of security and confidence to any implementation. The dynamics of the world we live in demand it. However, the road ahead is quite long, and we have much farther to go.

Bibliography

Adhami, R., & Meenen, P. (2001). Fingerprinting for security. *Potentials, IEEE, 20*(3), 33-38.

Ashbourn, J. (2004). *Practical Biometrics : From Aspiration to Implementation*. London: Springer.

Bannister, F. (2002). The Dimension of Time in Information Systems Research. *Electronic Journal of Business Research Methods, 1*(1).

Blackburn, T., Butavicius, M., et al. (2002). *Biometrics Technology Review 2002* (No. DSTO-GD-0359). Edinburgh, South Australia: DSTO Systems Sciences Laboratory.

Blyth, A., & Kovavich, G. L. (2001). *Information assurance : surviving the information environment*. London: Springer-Verlag.

Bolle, R. M., Connell, J. H., et al. (2004). *Guide to Biometrics*: Springer-Verlag.

Computer Security Institute / Federal Bureau of Investigation (CSI/FBI). (2003). Computer Crime and Security Survey. San Francisco, CA.

Computer Security Institute / Federal Bureau of Investigation (CSI/FBI). (2004). *Computer Crime and Security Survey*. San Francisco, CA.

Cummings, R. (2002). The evolution of information assurance. *Computer, 35*(12), 65-72.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*, 319-340.

Davis, F. D., Bagozzi, R. P., et al. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science, 35*, 982-1003.

Department of Defense. (2002). *DoD Directive 8500.1 Information Assurance (IA)*.

Department of Defense. (2003). *DoD Instruction 8500.2 Information Assurance (IA) Implementation*.

Department of Defense Joint Chiefs of Staff. (1998). *Joint Publication 3-13 Joint Doctrine for Information Operations*. Washington: Pentagon.

Department of Defense Joint Chiefs of Staff. (2001). *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*. Washington: Pentagon.

Dunstone, E. S. (2001). *Emerging biometric developments: identifying the missing pieces for industry.* Paper presented at the Signal Processing and its Applications, Sixth International, Symposium on. 2001.

Gamassi, M., Lazzaroni, M., et al. (2004). *Accuracy and performance of biometric systems.* Paper presented at the Instrumentation and Measurement Technology Conference, 2004. IMTC 04. Proceedings of the 21st IEEE.

Golfarelli, M., Maio, D., et al. (1997). On the error-reject trade-off in biometric verification systems. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 19*(7), 786-796.

Jain, A., Bolle, R., et al. (1999). *Biometrics : Personal Identification in Networked Society*. Boston, MA: Kluwer Academic Publishers.

Jain, A., Hong, L., et al. (2000). Biometric identification. *Association for Computing Machinery. Communications of the ACM, 43*(2), 90.

Jain, A., Ross, A., et al. (2004). An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on, 14*(1), 4-20.

Jain, A. K., & Uludag, U. (2003). Hiding biometric data. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 25*(11), 1494-1498.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical Research Planning and Design*. New York: Prentice Hall.

Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional, 3*(1), 27-32.

Mason, R. O., McKenney, J. L., et al. (1997a). Developing an Historical Tradition in MIS Research. *MIS Quarterly*.

Mason, R. O., McKenney, J. L., et al. (1997b). Developing an Historical Tradition in MIS Research: Steps and Assumptions. *MIS Quarterly, 21*(3), 307-320.

Matyas, V., Jr., & Riha, Z. (2003). Toward reliable user authentication through biometrics. *Security & Privacy Magazine, IEEE, 1*(3), 45-49.

McDowell, W. H. (2002). *Historical Research : A Guide*. London: Longman Publishing.

McHale, J. (2003). Biometrics: the body's keys. *Military and Aerospace Electronics*, 17-22.

Meenen, P., & Adhami, R. (2001). Fingerprinting for Security. *IEEE Potentials, 20*(3), 33-38.

Miller, B. (1994). Vital Signs of Identity. *IEEE Spectrum, 31*(2).

Nanavati, S., Thieme, M., et al. (2002). *Biometrics: Identity Verification in a Networked World*. New York: John Wiley & Sons, Inc.

Negin, M., Chmielewski, J., Thomas.A. , et al. (2000). An Iris Biometric System for Public and Personal Use. *Computer, 21*, 70-75.

O'Brien, J., Remenyi, D., et al. (2004). Historiography - A Neglected Research Method in Business and Management Studies. *Electronic Journal of Business Research Methods, 2*(2), 135-144.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2021-2040.

Ortega-Garcia, J., Bigun, J., et al. (2004). Authentication gets personal with biometrics. *Signal Processing Magazine, IEEE, 21*(2), 50-62.

Phillips, P. J., Martin, A., et al. (2000). An introduction evaluating biometric systems. *Computer, 33*(2), 56-63.

Prabhakar, S., Pankanti, S., et al. (2003). Biometric recognition: security and privacy concerns. *Security & Privacy Magazine, IEEE, 1*(2), 33-42.

Ratha, N. K., Connell, J. H., et al. (2001). Enhancing security and privacy in biometrics-based systems. *IBM Systems Journal, 40*(3), 614.

Reid, P. (2004). *Biometrics for Network Security*. Upper Saddle River, NJ: Prentice Hall.

Rejman-Greene. (2001). Biometrics -- Real Identities for a Virtual World. *BT Technology Journal, 19*(3), 115-121.

Ribaric, S., Ribaric, D., et al. (2003). Multimodal biometric user-identification system for network-based applications. *Vision, Image and Signal Processing, IEE Proceedings-, 150*(6), 409-416.

Seno, S., Sadakane, T., et al. (2003). *A network authentication system with multi-biometrics.* Paper presented at the Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on.

Uludag, U., Pankanti, S., et al. (2004). Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE, 92*(6), 948-960.

Woodward, J. D. (1997). Biometrics: privacy's foe or privacy's friend? *Proceedings of the IEEE, 85*(9), 1480-1492.

Woodward, J. D., Orlans, N. M., et al. (2003). *Biometrics: Identity Assurance in the Information Age*: McGraw-Hill.

Author's Vita

Master Sergeant Darren A. Deschaine enlisted in the United States Air Force and attended Basic Military Training at Lackland AFB, San Antonio, Texas in June, 1986. After initial training as a Cryptographic Maintenance technician, he was assigned to Lindsey Air Station, Wiesbaden, Germany as a communication technician. In September of 1990, he was reassigned to Kelly Air Force Base, San Antonio, Texas as a communication installation specialist for the 1827th Engineering and Installation squadron and a depot level secure communications maintenance technician at the Cryptologic Depot. He remained at this tour until August of 1995.

In September 1995, Master Sergeant Deschaine was reassigned to Biloxi, AFB Mississippi and was retrained as an Instrumentation and Telemetry Systems apprentice. Upon graduation in March 1996, he was transferred to Holloman AFB, Alamogordo, New Mexico where he was assigned duties as a Ground Support Crew chief for the 746 Test Squadron. After a two year tour, he accepted a special duty assignment to the National Reconnaissance Office in Chantilly, Virginia where he assumed duties as the Chief of the Technical Control Facility.

In August 2003, Master Sergeant Deschaine entered the Graduate School of Engineering and Management at the Air Force Institute of Technology. Upon graduation, he will be return to the engineering group at the National Reconnaissance Office in Chantilly, VA.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
01-03-2005	Master's Thesis	October 2003 – March 2005

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
An Analysis of Biometric Technology as an Enabler to Information Assurance	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	5d. PROJECT NUMBER
Deschaine, Darren A., Master Sergeant, USAF	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)	8. PERFORMING ORGANIZATION REPORT NUMBER
Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	AFIT/GIR/ENV/05M-03

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
National Defense University Information Resource Management College Fort Lesley J. McNair Washington, DC 20319-5066	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The use of and dependence on Information technology (IT) has grown tremendously in the last two decades. Still, some believe we are only in the infancy of this growth. This explosive growth has opened the door to capabilities that were only dreamed of in the past. As easily as it is to see how advantageous technology is, it is also clear that with those advantages come distinct responsibilities and new problems that must be addressed. For instance, the minute we began using information processing systems, the world of information assurance (IA) became far more complex as well. As a result, the push for better IA is necessary. To reach this increased level of IA, a further dependence on technology has developed. As an example, the field of biometrics has matured and has become an enabler to the United States Department of Defense IA model.

15. SUBJECT TERMS
Biometrics, Information Assurance, IA

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. David Bouvin, Captain, USAF
U	U	U	UU	75	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4742 (david.bouvin@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18